https://gospodarkainnowacje.pl

GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 28 | 2022

Economy and Innovation
ISSN: 2545-0573

ОПИСАНИЯ И СХЕМЫ ЗЛОУПОТРЕБЛЕНИЯ VOIP ШЛЮЗОВ И IP ТЕЛЕФОНИИ В ТЕЛЕФОННЫХ МОШЕННИЧЕСТВАХ

Хамдамов Голибжон Толибжонович

Майор в УВД Бухарской области, Узбекистан

ARTICLEINFO.

Ключевые слова:
IP телефония, VoIP шлюз, виртуальный АТС, SIP-протокол, телефонные мошенничества.

Аннотация

Телефонные мошенники появляются все чаще, поскольку современные технологии позволяют им без проблем находить своих жертв и зарабатывать неплохие деньги на их наивности. В данной работе ставится цель обсудить и проанализировать средства и способы совершения таких преступлений, а также даются предложения по борьбе против них.

Вступление

Технологии развиваются, упрощая нам жизнь. А вместе с ними в ногу со временем идут и мошенники. О многих их схемах уже известно широкой общественности, поэтому с каждым днем они придумывают все более хитрые способы выудить деньги. Один из широко распространённых видов таких действий - телефонное мошенничество используется для совершения преступлений в сфере телефонной связи. В этом виде мошенничеств главным залогом их благополучия являются спец оборудования данной сферы, описания и схемы злоупотребления, которыми приводятся далее.

Когда актуальность и востребованность IP-технологий в корпоративном секторе стала очевидна, производители офисных телефонных станций начали выпуск плат расширения для офисных АТС. Эти платы позволяли осуществлять передачу трафика напрямую в IP-сети. Однако стоимость плат расширения оказалась неоправданно высока, что и привело к появлению VoIP-шлюзов на рынке.

VoIP шлюз — это межсетевой шлюз, предназначенный для перевода голосового трафика между сетями традиционной телефонии и сетью передачи данных. VoIP-шлюзы можно разделить по типу телефонного стыка на цифровые и аналоговые. VoIP шлюзы могут иметь различную ёмкость, отличаться конструкцией и блоком питания (встроенный или внешний). VoIP шлюз, как правило, имеет встроенный маршрутизатор, поддерживающий широкий набор протоколов маршрутизации, авторизацию пользователей с возможностью автоматического получения и раздачи IP-адресов (как сервер и как клиент), установления приоритетов для различных видов и имеющий достаточный набор функций управления полосой пропускания, сетевой безопасности, учёта и анализа трафика и администрирования.

Основная часть

Основные отличия VoIP-шлюзов от плат расширения АТС:

- стоимость VoIP-шлюзов в несколько раз ниже (в расчёте на один канал);
- расходы на установку, настройку и обслуживание VoIP-шлюзов заметно ниже (за счет того, что эти работы могут выполняться силами собственной IT службы);
- увеличение числа каналов VoIP-шлюзов также обходится в несколько раз дешевле (докупаются модули расширения);
- VoIP-шлюзы лучше совместимы с VoIP-оборудованием других производителей (заметно меньше вероятность проблем при стыковке с оборудованием оператора IP-телефонии).

Часто VoIP-шлюз также называют SIP шлюзом или голосовым шлюзом, так как именно он кодирует и декодирует голос при передаче через SIP-протокол.

На первый взгляд может показаться, что голосовой шлюз для IP-телефонии выполняет только техническую задачу. На самом деле, данное устройство позволяет компаниям решать ряд бизнес-задач:

Переход на более качественную и выгодную связь.

Подключая корпоративные телефоны к IP-сетям, повышается качество телефонии. Вызовы без задержек идут через интернет. Во время разговора нет эха и помех. При этом звонки по многим направлениям становятся более выгодными.

Сокращение расходов на оборудование.

Не надо покупать специальные IP-телефоны. Любой аналоговый телефон и аппарат стандарта DECT доступны для подключения к IP-телефонии. Внедрение SIP-шлюза происходит в течение 1 рабочего дня, его можно подключить к корпоративной виртуальной АТС.

Бесплатные звонки внутри единой сети.

Если все телефонные номера сотрудников с помощью VoIP-шлюза подключены к IP-сети и одной виртуальной АТС, то можно создать единую корпоративную телефонную сеть. Звонки внутри компании не тарифицируются, даже если сотрудники находятся в разных городах.

Мониторинг звонков и разговоров.

Компании подключают аналоговые телефоны к IP-сетям и переходят на IP-телефонию, чтобы иметь возможность анализировать звонки и контролировать телефонные разговоры. Виртуальная АТС позволяет вести статистику и запись звонков, настраивать IVR, сценарии звонков.

Результаты и обсуждения

Надо принимать во внимание что это технология «двойного назначения». Её можно использовать и во благо, и во зло. Например, когда вам звонят доставщики еды, вы видите единый номер компании, а не реальный номер курьера. Агрегаторы такси, банки, турфирмы и другие сервисы такого рода входят в ряд таких случаев. В общем, это компании, которые решили поиграть в заботу о пользователе.

Когда придумывали стандарты связи, в приоритете было, чтобы всё заработало. Вопроса безопасности не стояло. В итоге, её прикручивали на ходу, а не внедряли при проектировании. Эту логику легко проследить на примере интернета: сперва сделали http, а потом придумали SSL-сертификаты с удостоверяющими центрами, чтобы получить более-менее безопасное httpS.

Подмена идентификатора, звонящего (CallerID spoofing) через виртуальную АТС, способствует

киберпреступникам в совершении телефонных мошенничеств. На самом деле всё проще в реализации. Для подмены номера достаточно иметь современные IT навыки, быть оснащенным соответствующей техникой и вложить немного денег. Например, в функционале бота в приложении Телеграм, возможно даже подменить голос.

Сегодня сильно распространено телефонное мошенничество, когда злоумышленники дозваниваются на номер случайного пользователя, чтобы обманным путем получить деньги. Чаще всего мошенники представляются сотрудниками банковского учреждения, выманивая реквизиты пластиковых карт. Однако такая схема постепенно устаревает — пользователи проявляют бдительность, не обращая внимания на подобные телефонные звонки.

К сожалению, злоумышленники постоянно придумывают новые способы незаконного получения дохода. Например, пытаются связаться с потенциальной жертвой под видом мобильного оператора. Абоненты обычно доверяют представителям компании, сообщая запрашиваемую персональную информацию. Результатом является обнуление баланса телефона или кража банковских реквизитов.

Телефонный спам может доставить серьезные неудобства, но не идет ни в какое сравнение с серьезным мошенничеством, цель которого – не просто прорекламировать услугу и найти клиентов, а обмануть и украсть деньги с банковского счета. Выясняем, как злоумышленники находят номера пользователей, а также разбираемся, каким образом это предотвратить.

Чтобы не стать жертвой мошенников или даже избежать звонков и сообщений от них, владельцу телефона следует прислушаться к таким рекомендациям:

- Как только во время разговора у пользователя появились подозрения, что ему звонит не сотрудник банка, а злоумышленник, нужно повесить трубку. А уже потом перезвонить в финансовую организацию (номера «горячей линии» легко найти на ее сайте и даже на банковской карте) и уточнить наличие звонка;
- Если деньги просят от лица знакомых или родственников, следует связаться с ними – и уточнить информацию. Впрочем, такие просьбы оказываются мошенничеством почти в 100% случаев;
- Нежелательно оставлять свои номера на площадках для объявлений, в анкетах и при регистрации на сайтах. Если без этого не обойтись, лучше завести отдельную сим - карту, которая будет использоваться только при необходимости (например, на период продажи автомобиля). Учитывая, что большинство смартфонов оснащено слотом для двух сим - карт, завести второй номер – не проблема;
- Если данные карты (даже если только номер) каким-то образом оказались у злоумышленников, ее стоит на всякий случай заблокировать. То же самое рекомендуется сделать, получив сообщение о списании средств за покупку, которую владелец карты на самом деле не совершал;
- Если мошенник вам все же позвонил, а вы его «рассекретили» - добавьте его номер в черный список. Так он точно не сможет вам перезвонить – по крайней мере, с того же телефона;
- Также не стоит устанавливать на смартфон и компьютер приложения из неизвестных источников, переходить по сомнительным ссылкам и получать права «суперпользователя». Все это делает гаджет уязвимым к вирусам и увеличивает вероятность попадания данных в чужие руки;
- заведите отдельную сим-карту для временной регистрации на сайтах;
- Все профили, в которых указан телефон, следует надежно защищать сложными паролями. А еще лучше – с помощью двухфакторной аутентификации, при которой получить доступ к

банку можно только после ввода дополнительного кода из СМС.

Заключение

Мошенничество рассматривает как противозаконное действие, которое сурово наказывается. Но даже несмотря на это, многие считают, что защититься от телефонного мошенничества сложно. И это действительно так. Хотя определенные меры есть.

Как вы могли убедиться, телефонное мошенничество включают в себя широкий диапазон незаконных деяний, начиная от мошенничества и заканчивая с кражей персональной информации. Важно понимать, что телефонные киберпреступления всегда ассоциируются с изощренными схемами и затрагивают «глубокий интернет». Наилучший метод защиты от кибератак – быть в курсе современных вышеупомянутых угроз.

Список литературы:

1. Белозерцев, С. М. Профилактика мошенничеств с использованием мобильных устройств и банковских карт в Иркутской области: проблемы и пути их решения. Вестник Восточно–Сибирского института МВД России. – 2015. – № 4 (75). – С. 9–14.
2. Волеводз, А. Г. Следы преступлений, совершаемых в компьютерных сетях, Российский следователь. – 2002. – № 1. – С. 4– 12.
3. Khamdamova, S. B. (2022). HARMONY OF TRADITION AND NOVELTY IN ENGLISH POETRY. CURRENT RESEARCH JOURNAL OF PHILOLOGICAL SCIENCES (2767-3758), 3(05), 69-72.
4. Khamdamova Sitora Bakhshilloyevna & Yusupova Hilola Uktamovna. (2021). SYMBOLISM IN WILLIAM BUTLER YEATS' POETRY. CENTRAL ASIAN JOURNAL OF LITERATURE, PHILOSOPHY AND CULTURE, 2(5), 131-135.
5. Гаджиев, М. С. Криминологический анализ преступности в сфере компьютерной информации. – Махачкала, 2004. – С. 81–85.
6. Дремлюга, Р. И. Международно–правовое регулирование сотрудничества в сфере борьбы с Интернет–преступностью Библиотека криминалиста. − 2013. − №5(10). – С.339–346.
7. Зыков, Д. А. Виктимологические аспекты предупреждения компьютерного мошенническтва. Владимир, 2002. – С. 156–165.
8. Mansfield–Devine S. «Darknets». Computer Fraud & Security. – 2009 (12). – P. 4–6. [Электронный ресурс] // Режим доступа: doi:10.1016/S1361–3723(09)70150–2
9. https://mobile-review.com/all/articles/analytics/kak-zashhitit-sebya-ot-telefonnyh-moshennikov-priemy-i-sposoby/
10. https://media.mts.ru/technologies/197260-kak-raspoznat-telefonnogo-moshennika/
11. https://www.tadviser.ru/index.php/Статья:Телефонное_мошенничество
12. file:///C:/Users/NoteService/Downloads/telefonnoe-moshennichestvo.pdf
13. Khamdamova, S. B. (2021). Early period of William Butler Yeats' poetry. ACADEMICIA: An International Multidisciplinary Research Journal, 11(3), 1587-1591.
14. Khamdamova, S. B. (2020). Interpretation of antonomasia in the translations of Abdulla Kadiri's Novel" Days Gone By". Electronic Journal of Aktual Problems of Modern Science, Education And Training. June,-III. ISSN.

15. Bakhshilloyevna, K. S., & Uktamovna, Y. H. (2021). SYMBOLISM IN WILLIAM BUTLER YEATS'POETRY. CENTRAL ASIAN JOURNAL OF LITERATURE, PHILOSOPHY AND CULTURE, 2 (5), 131-135.
16. Bakhshilloyevna, K. S. (2021). FORMATION OF MODERN ENGLISH POETRY IN THE LATE XIX AND EARLY XX CENTURIES. Euro-Asia Conferences, 1 (1), 459–461.
17. Khamdamova, S. B. (2022). HARMONY OF TRADITION AND NOVELTY IN ENGLISH POETRY. CURRENT RESEARCH JOURNAL OF PHILOLOGICAL SCIENCES (2767-3758), 3(05), 69-72.